330.10

Local WIC Agency Data System Guidelines

Overview

Introduction

Local WIC agencies must have safeguards in place to assure that participant information, food instruments, and equipment are secure. A local WIC agency data system security plan should be in place and reviewed each year. Appropriate changes should be made to the plan as needed.

Focus

Local WIC agencies are required to use and document clinic services and program benefits in the Focus data system. The applicant may not substitute any other data system for the Iowa WIC Program. Local WIC agencies are expected to establish routine procedures to assure the security and quality of electronic records, food instruments and data reports. State WIC office staff will also conduct data system reviews on a regular basis.

Local agency computer support

Local WIC agencies are required to have access to local computer support services to assist with troubleshooting local hardware and internet access issues. This may be agency staff or a contract with a local computer company.

Theft or damage

Theft or damage of data system equipment should be reported to the state office immediately. Computers/devices supplied by a local agency, or other third party entity, shall be wiped using a DoD approved process when no longer used with the Focus application.

In this policy

This policy contains the following sections

Clinic Safeguards

Physical site check

Local agency staff should periodically review their physical locations to determine if equipment or food instrument stock is in any potential danger. Review area for:

- Windows or doors that may be left open that could lead to theft opportunities or damage by weather,
- Windows or doors that leave equipment or records in full view, and
- Exposed water pipes or drain areas that could leak on equipment or materials.

WIC data system equipment

The following safeguards must be in place:

- WIC data system equipment is not to be used for personal use;
- Do not open or download personal files and visit only work-related websites. Visiting certain websites and/or downloading certain files can contain viruses that can harm the computer.
- Computers are locked in a cabinet or in a limited access area when not in use;
- When traveling to satellite clinics, laptops and printers should not remain in an unattended vehicle or overnight;
- To protect against electrical spikes and to keep systems from shutting down prematurely, surge protectors or uninterrupted power supply units should be used;
- When transporting equipment, laptops and printers should be carried in appropriate bags or containers;
- Quarterly cleaning of equipment; and
- Practice good house keeping with data system equipment. Encourage regular use of canned compressed gas on keyboards, printers, and intake/exhaust ports;

Food instruments

Local WIC agency staff must assure that theft or destruction has not occurred to food instruments. This includes:

- Storing all food instrument in a secure or limited access area during non-distribution, and
- Securing all food instrument stock out-of-sight and out-of-reach of participants and never left unattended during clinic.

Continued on next page

Clinic Safeguards, Continued

Participant records

All WIC participant information must remain confidential. This includes:

- Not displaying electronic participant records on the screen while the computer is unattended;
- Shredding WIC participant information that is no longer needed; and
- Not allowing non-WIC staff to have access to the WIC data system.

Continued on next page

Security Access/Tokens

Policy

Local and state WIC staff must use their assigned token when accessing the train and production environments of the data system**.** Staff shall not use a token assigned to another staff as it is your electronic signature within the data system.

Access levels

To assure program and data integrity of the WIC data system, there are multiple levels of security access. Data system security access is determined by position and clinic responsibilities. Access levels include:

- Scheduler-only,
- Support Staff,
- Health professional, non-CPA,
- CPA,
- Support Staff Admin,
- CPA Admin,
- Breastfeeding Peer Counselor
- IWIN Coordinator.

Token requests

WIC coordinators must fax **OR** mail an **IWIN Token User Information Form** and a **signed New User Request Form** to the WIC HelpDesk when new staff is hired. If the local agency has a token from a vacated position, an IWIN Token User Information Form and signed New User Request Form must be completed each time an individual is hired in that position. This includes staff who may have left the agency and then returned at a later date. The WIC HelpDesk will contact the WIC Coordinator when the token is activated and ready for use.

Token receipt

The Acknowledgement of Receipt of Security Token form will be mailed with the new token. If the staff member already has a token, this form will be e-mailed. This form must be reviewed, signed, and dated by the token user. The completed form must be be mailed, faxed, or e-mailed to the WIC HelpDesk.

Cost of tokens

Token licenses are paid by the state WIC office for local agency staff positions paid ≥ .2 FTE from WIC grant funds. The token license fee for IWIN user positions paid with < .2 FTE WIC grant funds is $60. Payment is due within 60 days of receipt of the token and invoice. Refer to the bottom of the invoice for proper payment instructions. The state WIC office reserves the right to approve or disapprove token requests.

Passwords and soft pins

Strong passwords shall be used with all computers/devices. Passwords and soft pins should be kept in a secure area. Local agencies must report any breech of password of security within 24 hours to the state WIC office.

Continued on next page

Security Access/Tokens, Continued

Lost or damaged tokens

WIC staff must report lost or damaged tokens immediately to the WIC HelpDesk. The WIC coordinator or lead WIC staff must complete and mail or fax a Token Replacement Request Form. When mailing back a damaged token, return it in a padded envelope to protect it from being damaged in the mail. Also, mail a copy of the Token Replacement Request Form along with the damaged token. The state WIC office will replace tokens as soon as possible.

Note: It is imperative that local WIC staff not share tokens and passwords while working in the train and production environments of the data system. Staff must use their assigned tokens.

Replacements

Replacement security tokens cost $60. It is the agency's discretion as to whether it is the agency or the staff person who will assume that cost.

Spare token

Each agency has a spare token that can be used if a staff person's token has become lost, damaged, or defective. Submit a Token Replacement Request Form and call the WIC HelpDesk to activate the spare token. This spare token will become the staff person's token. A new spare token will be provided. The spare token should only be used for emergencies and should not be used for a new user.

Note: The replacement cost applies for lost or damaged tokens. There is no cost to replace a token that has become defective.

Inactivate token

Upon the resignation of local agency staff, the WIC coordinator or lead WIC staff must complete and submit an Inactivate User Request Form to the state WIC office. The local agency may keep the token if the intent is to fill the position. The local agency will submit a WIC Token User Information Form and signed New User Request Form when the position is filled. If a staff member leaves the agency and then returns at a later date, a WIC Token User Information Form and New User Request Form must be completed. If the position is not filled, the token must be returned to the state WIC office with the Inactivate User Request Form.

Changes

If WIC staff have a change of name or change of IWIN rights, the WIC coordinator or lead WIC staff must complete and mail or fax the User Change Request Form to the state WIC office.

Location of forms

Token forms are found on the WIC Web Portal.

Data System Hardware, Software, and Internet Connectivity Requirements

Software

The following are software requirements:
- Anti-virus software
- Latest version of Adobe Reader and Internet Explorer
- Microsoft. NET Framework 1.1 with all service packs and security updates
- Microsoft .NET Framework 4.0 or higher.

Hardware

The following are agency hardware requirements:
- Minimum: Pentium Dual Core 2.6 GHz Processor, 2 GB of RAM, 80 GB Hard drive
  Recommended: Pentium 15 2 GHZ or greater processor, 4 GB of RAM or great, 160 GB hard drive or greater.

Windows Operating System

Local agencies must have the minimum Windows operating system requirements:
- Windows 7, service pack and current updates or higher

Note: Windows XP operating system is not supported.

Internet access

All WIC offices (includes split offices within an agency) must maintain high-speed Internet access. All WIC clinics must maintain Internet access. Connection to the Internet must meet the eWIC online system and Focus requirements.

Local agencies must have the minimum for Internet access:
- Bandwidth 1.5 mb

The following Internet access is recommended:
- 12mb Cable modem, 7 mg DSL modem, cellular (1.5mb or higher, or 4G (cellular)

Note: The following website lists cellular hotspots that are compatible with the Cradlepoint router. Go to the website and click on “Modem & Accessory Info”.

http://www.cradlepoint.com/products/small-business-home-office-routers/mbr1200b-small-business-mobile-broadband-router

Contact the WIC HelpDesk if internet service changes at any WIC clinic.

Data System Hardware, Software, and Internet Connectivity Requirements, Continued

IDPH provided security software (HEAT)

IDPH-provided security software (HEAT) is required on ALL computers/devices running the Focus suite of applications.

IDPH-provided computers/devices will come with security software preinstalled and configured. The security software shall be set for automated reporting to IDPH. Only approved software will be allowed to run on IDPH-provided computers/devices utilizing the Focus suite of applications. An application whitelist will be used to secure endpoints involved in EBT processing including devices with card readers and pin pads. IDPH shall monitor for and investigate attempts to install non-approved software.

Local agency supplied computers/ devices

Computers/devices supplied by a local agency or other third party entity running the Focus suite of application must be approved by IDPH. Local agency and third party computers/devices must run the security software (HEAT). Installation of the Focus software allows for continuous monitoring by IDPH. IDPH may contact a local agency in response to alerts generated by the security software.

IDPH reserves the right to remove computers/devices that are not secure from Focus application participation without notice. Tampering with security software settings is prohibited.

eWIC devices

At no time shall eWIC related components including devices with card readers and pin pads, be attached to computers/devices supplied by a local agency or other third party entity. Computers/devices supplied by a local agency or other third party entity running the Focus suite of application must be approved by IDPH. Local agency and third party computers/devices must run the security software HEAT. Installation of the Focus software allows for continuous monitoring by IDPH. IDPH may contact a local agency in response to alerts generated by the security software.

E-mail

All agency executive directors, WIC Program coordinators, and lead staff in a split agency key must have **individual** e-mail addresses with the capacity to send and receive electronic communications (e-mail and attachments).

All agency staff using IWIN must have the ability to use local agency e-mail to contact the WIC state office. This can be a group of individual e-mail address. Local agency staff is not allowed to e-mail the state WIC office with personal e-mail accounts from state owned computers.

Continued on next page

Data System Hardware, Software, and Internet Connectivity Requirements, Continued

Local computer support	Local WIC agencies are required to provide local agency computer support and maintenance of local hardware and operating software. If state-owned WIC computers are put on local agency networks, the local agency is responsible for printer connectivity, Internet connectivity, triaging network issues and configuring replacement hardware.
State-supplied data system equipment	The state WIC office will supply data system equipment to local WIC agencies based on workload and caseload. The state WIC office periodically evaluates these determinants and reserves the right to recover that equipment so it can be redistributed to other WIC contractors. The state WIC office will replace WIC data system equipment on a scheduled basis (budget permitting). Local agencies should contact the WIC HelpDesk if replacement or additional equipment is needed. Local WIC agencies must maintain insurance coverage for data system equipment being used in their agency.
Network Downtime (NDT) mode	Network Downtime (NDT) mode is for use if for some reason the clinic does not have access to the Internet. NDT mode should only be used in very rare circumstances. If a clinic uses NDT mode, there would no ability for participants to be issued a card or benefits during the clinic. Also, when a clinic uses NDT mode, the clinic must stay in NDT mode for the remainder of the clinic day. The WICHelpDesk must be notified before a clinic uses NDT mode.

Local Agency Security Plan

Local agency security plan

A local agency security plan must include:

- Measures for securing equipment, food instruments, and electronic participant records;
- Assurances that staff are using their assigned security token;
- Assurances that WIC participant information remain confidential;
- A record of emergency preparedness procedures related to the data system; and
- A physical site checklist related to the present clinic sites.

Personnel practices

At the beginning of employment, coordinators must discuss confidentiality of records and safeguarding of equipment with staff. A signed Statement of Confidentiality is recommended at the time of hire.

If an employee is dismissed, they should return their security token and have no further access to participant records or agency equipment. The WIC coordinator must submit an Inactivate User Request Form to the WIC HelpDesk. Coordinators are encouraged to maintain a record of accesses given to employees.

This page intentionally left blank.